Corporate Account Takeover

Corporate account takeover is when cyber thieves gain control of a business' bank account by stealing the business' valid online banking credentials.

Although there are several methods being employed to steal credentials, the most prevalent involves malware that infects a business' computer workstations and laptops. Cyber thieves use the online banking sessions to initiate funds transfers, by ACH or wire transfer, to the bank accounts of associates within the U.S.

- **Why are small businesses and organizations targeted?**
  - Small businesses often do not have the same level of resources as larger companies to defend their information technology systems.
  - Many small businesses do not monitor and reconcile their accounts on a frequent or daily basis.
  - Small businesses bank with a wide variety of financial institutions with varying degrees of IT resources and sophistication.

- **Prevention, detection and reporting for business customers account control:**
  - Reconcile all transactions on a daily basis.
  - Initiate ACH and wire transfers under dual control, with a transaction originator and a separate transaction authorizer.
  - Utilize routine reporting on transactions.
  - Perform risk assessment of banking products/ services; including; regular reviews of user access levels, dollar limits and activity.
  - Immediately report any suspicious transactions to the financial institution.
  - Stay in touch with other businesses and industry sources to share information regarding suspected fraud activity.

- **Computer security tools and practices**
  - Install a dedicated, actively managed firewall to limit the potential for unauthorized access to a network and computers.
  - Install commercial anti-virus software on all computers.
  - Ensure virus protection and security software are updated regularly.
  - Ensure computers are patched regularly, particularly operating system and key applications, with security patches.
  - Install spyware detection programs.
  - Be suspicious of emails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. If you are not certain of the source, do not click any links.
  - Limit administrative rights on users' workstations.
  - Carry out all online banking activities from a stand-alone computer system from which email and web browsing are not possible.
  - Verify use of a secure session ("https") in the browser for all online banking.
  - Never access bank, brokerage or financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.

Corporate Account Takeover PG. 2

- **Recommendations for what to do if you become a victim of corporate account takeover:**
  - Immediately cease all activity from computer systems that may be compromised. Disconnect the Ethernet or other network connections to isolate the system from remote access.
  - Immediately contact your financial institution and request assistance with the following actions:
    - Disable online access to accounts.
    - Change online banking passwords.
    - Open new account(s) as appropriate.
    - Request the financial institution's agent review all recent transactions and electronic authorizations on the account.
    - Ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address.
  - Maintain a written chronology of what happened, what was lost and the steps taken to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.

Listed below are a few suggestions for employers and employees to consider both at and outside the workplace to prevent account takeover.

- Create strong passwords.
- Change passwords frequently.
- Never share username and password information with third-party providers.
- Never leave a computer unattended while using online banking or investing service.
- Prohibit the use of "shared" usernames and passwords for online banking systems.

  - File a police report and provide the facts and circumstances surrounding the loss. Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often facilitate dealing with insurance companies, banks and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.

If you become suspicious, immediately contact the authorities and United Bank of Iowa.

UNITED BANK of IOWA
The Difference is Here! Member FDIC

10/2013